PTO/SB/33 (07-05)
Approved for use through xx/xx/200x. OMB 0651-00xx
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional)
200205659-2

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)]

On December 26, 2007

Signature

Typed or printed name

Application Number	Filed
10/694,824	10/29/2003

First Named Inventor
Antonio LAIN

Art Unit	Examiner
2137	Techane Gergiso

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest.
See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)

☒ attorney or agent of record.
Registration number 26,874

☐ attorney or agent acting under 37 CFR 1.34.
Registration number if acting under 37 CFR 1.34

(Reg. 59597)
Signature
for /

William T. Ellis
Typed or Printed Name

(202) 672-5485
Telephone Number

December 27 2007
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☒ *Total of 1 forms are submitted.

This collection of information is required by 35 U.S.C. 132. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Antonio LAIN et al.
Title:	MANAGEMENT OF SECURITY KEY DISTRIBUTION
Appl. No.:	10/694,824
Filing Date:	10/29/2003
Examiner:	Techane Gergiso
Art Unit:	2137
Confirmation Number:	7594

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the New **Pre-Appeal Brief Conference Pilot Program**, announced July 11, 2005, this Pre-Appeal Brief Request is being filed together with a Notice of Appeal.

Remarks/Arguments begin on page 2 of this document.

REMARKS

The rejections of record are untenable because none of the cited references, either alone or in combination, teach or suggest a method including the steps of (a) "issuing keys to users from domains within the hierarchy upon the basis of their grouping," or (b) "allocating keys to users which are indicative to a service provider of the level of service to which they are entitled," and (c) "for at least one level of service provision, allocating dummy keys which do not provide security for the provision of the service," as claimed.

The claims currently under examination, claims 1-14, stand rejected as follows:

1. under 35 U.S.C. § 103(a) as allegedly being unpatentable over U.S. Patent 7,039,803 to Lotspiech (hereinafter "Lotspiech") in view of U.S. Patent Application Publication 2002/0029337 to Sudia (hereinafter "Sudia"). See Final Rejection dated August 31, 2007.
2. under 35 U.S.C. § 103(a) as being unpatentable over Sudia in view of Lotspiech.

None of these references teaches or suggests (a) "issuing keys to users from domain within the hierarchy upon the basis of their grouping," (e.g. see claims 1, 13 or 14), (b) "allocating keys to users which are indicative to a service provider of the level of service to which they are entitled," and (c) "for at least one level of service provision, allocating dummy keys which do not provide security for the provision of the service." (e.g. see claim 10). See final Office Action dated August 31, 2007. (hereinafter "OA").

The invention as claimed groups users of a service within a hierarchy. Keys are issued from a domain, or according to a level of service the user is to be provided. This enables one group of users, for example low value users that subscribe to a lower level of service, to have less of an effect on another group of users, for example high value users that subscribe to a higher level of service. The result may be that low value users may experience the inconvenience of key reissue more frequently than the higher value users. Further, decisions may be taken to ignore invalidation in the low value user group with only a relatively low likelihood of compromise of the higher value services due to the distinct positioning of domains within the cryptographic hierarchy.

First, the Examiner cites Lotspiech as teaching "issuing keys to users from domains within the hierarchy upon the basis of their grouping." (OA, page 5, line 9) However, there is no teaching or suggestion that a key is issued to a user **from a domain within the hierarchy**, based upon the user's grouping. Rather, Lotspiech teaches that users are grouped into possibly

overlapping subsets, with each subset having a unique key, and each user assigned respective private information I_u. (Lotspiech, column 3, lines 11-14) Lotspiech teaches:

> "A user's **private information I_u** is preferably found as information i_j in a transmitted message that indicates that a user belongs to a subset S_{ij} of one of the groups... A subset key L_{ij} can then be obtained from or derived using the private information of the user" (Lotspiech, column 3, lines 29-34)

This private information I_u can be supplied by the system, (Lotspiech, column 6, lines 41-43). and consists of the receiver's position in the tree and the subset keys associated with its ancestor nodes. (Lotspiech, column 8, lines 23-26). Thus, there is no teaching or indication in Lotspiech that the private information assigned to the user is based upon their grouping. Rather, the private information is obtained from the labels of nodes that are not in direct path between the receiver and the root node, and is associated with more than one subset. Thus, if the user is in a certain group, which is in a specific domain of the hierarchical tree, the labels would be obtained from an ancestor of the receiver node. Thus, the labels utilized to make the private information assigned to the user are not derived from associations of the user, but rather from nodes that are explicitly NOT associated with the user. There is no indication in Lotspiech that the labels are obtained from the domain in which the receiver resides. Rather, Lotspiech seemingly teaches the opposite – that the labels would be obtained by nodes "that 'hang' off the direct path and are inducted by some node vi, and ancestor of u." (Lotspiech, column 10, lines 3-10) Thus, Lotspiech clearly fails to teach "issuing keys to users from domains within the hierarchy upon the basis of their grouping." (claim 1) Thus, in Lotspiech, the users are partitioned into disjoint subsets that have associated subset keys, but there is no indication that the users are assigned keys. Rather, the users are assigned private information that is utilized to decrypt the subset keys (Lotspiech, column 6, lines 41-53).

Correspondingly, Lotspiech also fails to teach "allocating keys to users which are indicative to a service provider of the level of service to which they are entitled." (claim 10) There is no teaching or suggestion in Lotspiech that the private information I_u contains any information that indicates to a service provider the level of service to which a user is entitled. As shown above, there is no indication or teaching in Lotspiech of allocating a key to a user based upon the associations or groupings of that user.

Second, Sudia fails to teach "issuing keys to users from domains within the hierarchy upon the basis of their grouping." (claim 1) Sudia teaches the use of digital signatures and public-

key certificates. Specifically, Sudia states that a Certification Authority (CA) signs a public key of a user that bind a user's name to the public key. (Sudia, paragraph 0013) There is no teaching or suggestion in Sudia of issuing keys to users, let alone that a key is issued to a user from a domain. Rather, the key, in association with a public-key certificate, is certified by a CA. Thus, the user already has a key that has been issued. The specific ways in which keys are issued are not addressed in Sudia; rather, well-known cryptographic systems are discussed which explain how keys are obtained and/or utilized. There is no teaching or suggestion in these systems, or in Sudia, that a key is issued to a user from domains within the hierarchy. Thus, Sudia also fails to teach this feature of the invention as claimed,

Third, the Examiner cites Sudia as teaching "allocating keys to users which are indicative to a service provider of the level of service to which they are entitled." (claim 10) (OA, page 9, lines 7-8) The Examiner then cites column and line numbers to teach this feature, supposedly of Sudia. However, Applicants note that Sudia is a Patent Application Publication, which is structured in paragraph form. Thus, this citation is clearly in error.

Applicant could not find any relevant teaching in Sudia as to allocating keys to users. As noted above, Sudia teaches binding public keys to users. There is no teaching or suggestion of allocating or issuing keys in Sudia, let alone allocating keys that are indicative to a service provider of a level of service to which the user is entitled. Thus, Sudia clearly fails to teach this feature of the invention as claimed.

As mentioned, Lotspiech also fails to teach this feature. There is no teaching of service providers in Lotspiech, or of indicating a level of service to which a user is entitled. Further, there is no teaching or suggestion of allocating keys that would provide such an indication to a service provider. As mentioned above, Lotspiech teaches supplying a user with private information I_u that consists of its position in the tree and the subset keys associated with its ancestor nodes. (Lotspiech, column 8, lines 23-26). There is no mention or teaching that the private information includes an indication of a level of service to which the user is entitled. Lotspiech also fails to teach this feature of the invention as claimed.

Fourth, the Examiner asserts that "Sudia does not explicitly disclose for at least one level of service provision allocating placebo keys which do not provide security for the provision of the services." (OA, page 9, lines 9-10). Rather, the Examiner cites the session key K of Lotspiech to teach this feature. First, Lotspiech does not teach levels of service provision. Thus, Lotspiech would necessarily fail to teach allocating keys based upon a level of service provision.

However, even if the session key K were to be incorrectly interpreted as allocated for a specific level of service provision, the session key K is not a placebo key. Specifically, Lotspiech teach that the session key K is utilized to encrypt content that is broadcast in a message M. (Lotspiech, column 6, lines 54-57). Thus, the session key K is not a placebo key, because it provides security for the system of Lotspiech. There is no teaching or suggestion in Lotspiech of a key that does not provide security for the system. Thus, Lotspiech also fails to teach this feature of the invention as claimed.

Fifth, one of skill in the art would have been devoid of any motivation and reasonable expectation of success in combining the teachings of Lotspiech and Sudia. Lotspiech appears generally relevant to cryptographic keys generated from an ancestral hierarchy. Sudia is related to digital signatures. The Examiner contends this to be an 'analogous art'. However, digital signatures and cryptographic keys are two very different things which serve two very different purposes: keys protect and restrict access; whereas signatures authenticate. Thus, it is respectfully submitted that this combination would not occur to one of ordinary skill in the art of encryption and thus is not proper. Further, even if the combination were made, fundamental elements of the claims are missing from the combination.

Conclusion:

In view of the foregoing, it is respectfully submitted that the application is in condition for allowance. Applicants reserve the right to supplement these remarks and, should the application not be allowed, submit additional arguments in an Appeal Brief or at some later stage of prosecution.

At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 C.F.R. § 1.25. Additionally, charge any fees to Deposit Account 08-2025 under 37 C.F.R. § 1.16 through § 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees.

Respectfully submitted,

Date December 27, 2007

By [signature] (Reg 59597)

For William T. Ellis
Attorney for Applicant
Registration No. 26,874

HEWLETT-PACKARD COMPANY
Customer Number: 22879
Telephone: (202) 672-5300
Facsimile: (202) 672-5399